Protection of Confidential or Sensitive Information

The following are recommended, when practical, for the protection of confidential or sensitive information:

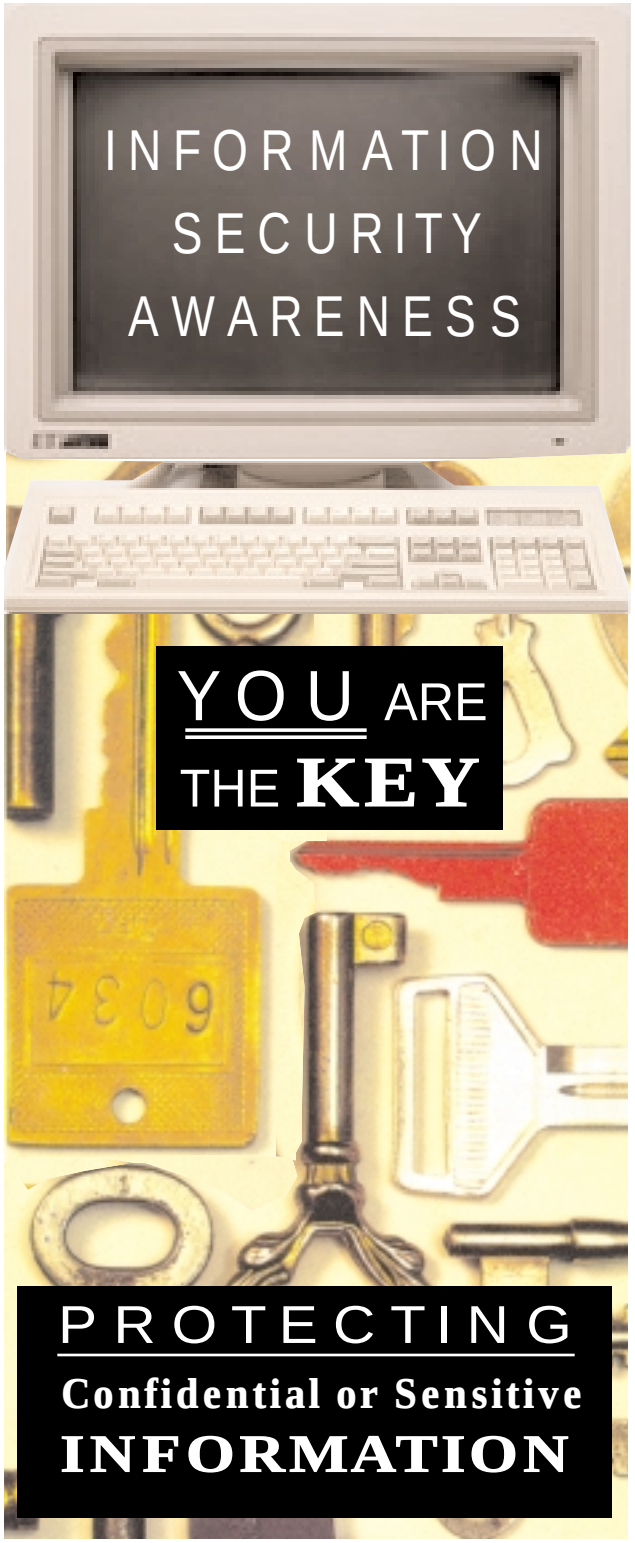
- When leaving the work area for a short period of time, put printed documents that contain confidential or sensitive information out of sight.
- When leaving the work area for an extended period of time, all confidential or sensitive material should be stored in locked cabinets, desks, or offices. Access should be restricted to authorized personnel only.
- Use double envelopes when sending confidential materials. The inside envelope should be sealed and clearly marked as being "CONFIDENTIAL".
- Confirm the identity of any individual who has requested confidential or sensitive data. Numerous scams exist that are used to get passwords, confidential information, personal information, etc. that the requestor intends to misuse.
- Do not disclose confidential or sensitive information unless permitted by statute or regulations.
- When there is a business need to discuss confidential information within the office, discuss the information in an enclosed room, if possible.
- Do not disclose confidential or sensitive information through telephone conversations unless the identity of the caller has been verified to be an individual who has legitimate access to the data. When in doubt, do not disclose any information. Seek assistance from appropriate staff in your organization.
- Log off from all networked systems that contain confidential or sensitive information whenever you leave your work area for an extended period of time.
- Take reasonable precautions to ensure that each fax containing confidential and sensitive material was appropriately received.
- Media containing confidential or sensitive information should be securely stored when maintained in automobiles, at home, or in the workplace.
- When encryption software is available, encrypt all confidential or sensitive information.

QUESTIONS?

Call the Information Security and Management Systems Branch at 657-3409

State of California
Gray Davis, Governor
Health and Human Services Agency
Grantland Johnson, Secretary
Department of Social Services
Rita Saenz, Director

PUB 311 (2/00)



Destruction of Confidential and Sensitive Information

DEFINITIONS

Data Remanence

Data remanence is the residual physical representation of data that has been in some way erased. After electronic media is erased there may be some physical characteristics that allow data to be reconstructed.

Degaussing

Degaussing of media is done by special equipment that erases the data from the media, leaving the surface in random patterns and rendering the data unrecoverable. Degaussing may require restoration of factory installed timing tracks.

Clearing

Clearing is the removal of information (typically by overwriting) assuring that the data may not be reconstructed using normal system capabilities.

Overwriting

Overwriting is considered to be an effective method of clearing data in an operational system when the media will stay within your organizational unit.

Purging

Purging is the removal of information in such a way that there is assurance that the data may not be reconstructed through open-ended laboratory techniques. Purging should be used when the secured physical environment of the media will not be maintained.

Hard Drives and Tapes

Be aware that system software (operating system software, application system software, etc.) is licensed as it exists on the machine. If a hard drive is going to be transferred to another organization, this licensed software needs to be securely removed unless the license is also being transferred. Failure to do this can result in licensing violations.

If degaussing equipment is available, degauss hard drives and tapes when they are going to be used outside of the organizational unit.

If degaussing equipment is not available, overwrite the confidential or sensitive data before allowing reuse of the hard drive or tape.

Floppy Diskettes

Floppy diskettes that contain confidential or sensitive data should not be used outside of the organizational unit. If they are no longer needed, they should be physically destroyed.

If floppy diskettes are going to be used within the organizational unit, overwrite the confidential or sensitive data before allowing reuse.

Solid State Components

Solid state components are erased through the use of ultra-violet light or some other sort of flash to erase/burn the information. If these lights are not available, you should physically destroy the solid state components.

Tapes

Where degaussers are available, use them to destroy data on tapes. Be sure to use a degausser that is appropriate for the type of tape being erased. Where degaussers are not available, the tape may be overwritten to destroy the data. Be aware that inter-record gaps may preclude proper clearing.

If neither of the above options is feasible, the tape must be destroyed.

Multiple Disk Units

Use the appropriate destruction technique for the type of media used in multiple disk units.

Optical Media

Optical media, such as CD-ROMS that contain confidential data should be broken.

Leased Equipment

Leased equipment should not be returned to the vendor until the data is securely destroyed. Contractual maintenance agreements should address the issue of degaussed media and its effect on equipment warranties.